

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

----- X
:
AMERICAN COLLEGE OF MEDICAL :
GENETICS AND GENOMICS :
:
:
Plaintiff, :
:
vs. : **COMPLAINT AND DEMAND FOR**
:
:
C SYSTEMS, LLC : **TRIAL BY JURY**
:
:
Defendant. :
----- X

Plaintiff American College of Medical Genetics and Genomics (“ACMG”), by and through its counsel, hereby alleges as follows for its Complaint against C Systems, LLC (“C Systems”):

NATURE OF THE ACTION

1. This is an action for damages stemming from a data breach that occurred as a direct result of C Systems’ substandard data security practices and failure to patch known vulnerabilities. C Systems’ data security practices violated the clear requirements of C Systems’ contractual obligations to ACMG in connection with C Systems’ provision of technology services to ACMG.

2. ACMG is a not-for-profit membership organization of medical geneticists, providing education, resources, and a voice for more than 2,400 clinical and laboratory geneticists, genetic counselors and other healthcare professionals, nearly 80% of whom are board certified in the medical genetics’ specialties. ACMG’s mission is to improve health through the clinical and laboratory practice of medical genetics as well as through advocacy, education and

clinical research, and to guide the safe and effective integration of genetics and genomics into all of medicine and healthcare, resulting in improved personal and public health.

3. C Systems is a software and technology service provider that, among other things, provides website and database development and management services.

4. In approximately March 2017, ACMG entered into two contracts with C Systems: *first*, a Master Consulting Agreement, and *second*, a Hosting Order. The Master Consulting Agreement (dated March 28, 2017) provides “the terms and conditions that govern individual written requests for consulting services (each “Task Order”).” The Hosting Order (dated March 16, 2017) provides that C Systems will supply servers and be in charge of managing the operation and the security of the iMIS software running on ACMG’s servers (including public-facing website and internal database). Specifically, among other obligations, the Hosting Order provides that C Systems will provide “Software hosting, which is keeping C Systems, iMIS, and related software on our servers, available for your use and providing update, maintenance and diagnostic services as part of your monthly hosting fee. Related software includes supporting software like backup and security programs and we maintain that software, as well. We will update the Software for you when updates are available and considered stable and necessary.”

5. Throughout the Request for Proposal (“RFP”) process, C Systems made numerous representations regarding the data security measures that C Systems had in place and would maintain throughout the time period in which C Systems provided services to ACMG in order to induce ACMG to purchase its services. For example, C Systems assured ACMG that its “premier hosting solution provides ... security required for all customers to prevent network threats from getting in – and spreading.”

6. Despite these representations and contractual commitments, C Systems failed to implement critical available Software updates, thereby allowing a third-party attacker access to ACMG's data hosted on servers maintained by C Systems from February 15, 2020 through May 1, 2020 (the "Data Breach"). Specifically, the attacker was able to exploit an unpatched vulnerability in the software run on ACMG's servers, allowing the attackers to add malicious code to ACMG's website and steal payment card numbers that had been entered on ACMG's website, www.ACMG.net.

7. Based on ACMG's investigation to date, the attacker could exfiltrate names, addresses, and payment card information of individuals who inputted that information via ACMG's website.

8. On approximately August 13, 2020, ACMG notified impacted individuals and relevant regulators about the Data Breach.

9. ACMG later learned that C Systems had not patched the iMIS software running on ACMG's servers with the latest updates **since October 2018** – even though numerous new security patches had been released. Nor had C Systems ever told ACMG of its outdated patches. In fact, a patch released in February 2019, but not applied to ACMG's software, contained upgraded security features that would have prevented the Data Breach.

10. The results of this Data Breach have been significant to ACMG, incurring over one hundred and fifty thousand dollars in costs necessary to investigate the Data Breach, provide notification to individuals, offer identity monitoring products to potentially impacted individuals, and provide notification to regulators.

11. C Systems now apparently claims that it was not responsible for ensuring the installation and implementation of software patches to ACMG's system in order to prevent

incidents like the Data Breach that occurred. However, ACMG retained C Systems based solely upon the specific and unambiguous representations made by C Systems that it would ensure that software patches were installed and implemented on ACMG's system to prevent threats like the Data Breach.

12. Accordingly, because of C System's actions, as described more fully below, C Systems violated its representations regarding data security, and ACMG is entitled to recover from C Systems all costs and expenses incurred by ACMG as a result of the Data Breach, and treble damages, as well as counsel fees and costs, pursuant to the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.*, and the applicable agreements between the parties.

THE PARTIES

13. Plaintiff ACMG is a not-for-profit organization with its principal place of business located at 7101 Wisconsin Avenue, Suite 1101, Bethesda, Maryland 20814.

14. Defendant C Systems is a New Jersey limited liability company with its principal place of business located at 510 Thornall Street, Suite 310, Edison, New Jersey 08837.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction under 28 U.S.C. § 1332, because there is complete diversity of citizenship between Plaintiff and Defendant, and the amount in controversy exceeds \$75,000 (not including interest and costs).

16. Venue is proper in this District under 28 U.S.C. § 1391(a) because C Systems has a place of business located in this District, a substantial part of the events giving rise to ACMG's claims occurred in this District, and the contract at issue provides, in relevant part, that "[t]he laws of New Jersey govern this agreement and you consent to the exclusive jurisdiction of the

federal and state courts of Middlesex County, New Jersey in any action arising from or related to this Agreement.”

FACTUAL ALLEGATIONS

C Systems’ Engagement

17. In late 2016, ACMG wished to engage a third-party vendor to assist with the development and maintenance of its databases and website, www.ACMG.net. This included both providing functional support to further develop its website, as well as providing the security for its website.

18. C Systems submitted a response to ACMG’s RFP, which detailed the services C Systems proposed to provide to ACMG. For example, C Systems’ response to the RFP included the guarantee that C Systems would provide the “security required for all customers to prevent network threats from getting in – and spreading”; “intercepting 15 million attacks a day”; and “monitoring, support, security included by default.”

19. C Systems made similar guarantees prior to executing the contract. For example, on November 7, 2016, in response to ACMG’s question (“Is ongoing routine maintenance (e.g. OS security updates, patches) included?”), C Systems’ account manager Keith Perigo wrote: “Yes, standard for all clients. Patch windows scheduled with you during on-board and security related updates pushed during this time. If Edge [Hosting]¹ determines you are vulnerable and require an update outside of scheduled window we will notify you and alert of update with option to decline.”

¹ Edge Hosting was a service provider hired by C Systems to assist with C Systems’ performance of its obligations to ACMG. In 2017, Edge Hosting was acquired by DataBank Ltd., who continued to serve as a service provider for C Systems.

20. Based on these guarantees, in approximately March 2017, ACMG entered into two contracts with C Systems: *first*, a Master Consulting Agreement, and *second*, a Hosting Order.

21. The Master Consulting Agreement (dated March 28, 2017) provides “the terms and conditions that govern individual written requests for consulting services (each “Task Order”).” The Master Consulting Agreement states that C Systems “will have access to certain trade secrets or other confidential information belonging to [ACMG], or belonging to third parties and which is in [ACMG’s] possession,” and obligated C Systems “not [to] disclose any such confidential information to any third party.” Exhibit C – Task Order to the Master Consulting Agreement states that “individual tasks will include: 1. Assist with the delivery and implementation of iMIS software, upgrades, and new releases. 2. Assist with day-to-day use, support, and configuration of the iMIS database... A C Systems project manager will be assigned to review all information systems needs.”

22. The Hosting Order (dated March 16, 2017) provides that C Systems will supply servers and be in charge of managing the operation and the security of ACMG’s iMIS database and website. The Hosting Order requires C Systems to provide “Software hosting, which is keeping C Systems, **iMIS**, and related software on our servers, available for your use and providing update, maintenance and diagnostic services as part of your monthly hosting fee. Related software includes supporting software like backup and security programs and we maintain that software, as well. We will update the Software for you when updates are available and considered stable and necessary.” The Hosting Order also warrants that C Systems “will provide you with the same level of service we provide to others.” Additionally, it provides that

“[w]e may subcontract some of our tasks, including the location of the equipment at a service center, but we shall remain liable to you for the performance of all subcontracted tasks.”

23. Early on, C Systems routinely notified ACMG when iMIS released a software upgrade or patch. Moreover, any security modifications to the application infrastructure needed to go through C Systems in order to be completed. For example, ACMG needed to contact C Systems in order to set up a VPN account in the firewall or to review the firewall rules. The same was true for applying any iMIS software upgrades or patches --- only C Systems had the ability to apply those upgrades to ACMG’s systems.

The Data Breach

24. On December 9, 2019, a development company named Progress publicly announced that its Telerik UI software contained a “critical vulnerability.” C Systems ran Telerick UI software on ACMG’s website, but did not alert ACMG to this vulnerability.

25. In April, 2020, ACMG noticed some abnormalities with the data in its database, and escalated the concern to C Systems on April 21st, asking them to investigate. Later that day, C Systems identified certain web bot activity creating fake accounts, but in response to ACMG’s inquiries of whether there were any security concerns, C Systems responded, in part, “no indication of any kind of SQL injection attempts or anything that struck [C Systems] as particularly nefarious.” But, as ACMG soon learned, this was not true – an unauthorized actor was active on ACMG’s database and servers maintained by C Systems.

26. On approximately April 28, 2020, ACMG became aware that an unauthorized actor may have been able to exploit a vulnerability in the software run on ACMG’s website. Upon discovering this, ACMG took prompt action to protect its systems, patch the vulnerability, and investigate.

27. ACMG's investigation determined that an unauthorized third party had accessed ACMG's database and servers maintained by C Systems containing ACMG data from February 15, 2020 through May 1, 2020 (the "Data Breach"). The attacker exploited a vulnerability on ACMG's servers, added malicious code to ACMG's website, and stole payment card numbers entered on ACMG's website.

28. On May 4, 2020, C Systems obtained the iMIS security patch from ASI, and on May 5, 2020, C Systems applied the iMIS security patch to ACMG's systems.

29. During the investigation of the incident, C Systems confirmed that, unbeknownst to ACMG, C Systems had not applied *any* security patches for over two and a half years — since a patch originally released in October, 2018 — even though numerous patches had been released in the interim (including some which specifically featured security patches).

30. Critically, the software manufacturer (ASI) represented that a security patch released in February 2019 contained mitigating components that would have prevented the Data Breach.

31. During ACMG's investigation, C Systems confirmed that it had applied the February 2019 security patch to its other customers' systems. However, C Systems did not apply this security patch to ACMG's systems, nor even tell ACMG about the availability of the security patch.

C Systems Refuses ACMG's Demand for Payment

32. After ACMG's investigation into the incident revealed that C Systems' inadequate data security measures and failure to patch were the primary causes of the attacker's ability to access the information of ACMG's members and other users, ACMG made due

demand on C Systems for reimbursement of the costs ACMG incurred to date as a result of the Data Breach.

33. C Systems has refused ACMG's demands and instead has forced ACMG to incur ongoing Data Breach response costs as well as to litigate these otherwise clear claims. Indeed, C Systems now claims that it was not responsible for ensuring that security patches were installed on ACMG's system, or notifying ACMG of potential vulnerabilities. This, however, is not only contrary to C Systems' contractual obligations, but also to its affirmative representations that were relied upon by ACMG in deciding to enter into a relationship with C Systems, as well as to C Systems' previous practice of notifying ACMG when iMIS released new patches.

CLAIMS FOR RELIEF

COUNT I –Breach of Contract

34. ACMG incorporates each of the above allegations as if set forth fully herein.

35. ACMG and C Systems entered into the Master Consulting Agreement and Hosting Order in March 2017. Both agreements went into effect then and remained in effect until after the Data Breach was discovered by ACMG.

36. ACMG performed under both agreements in all respects, including by tendering all payments due to C Systems under both agreements during the period it was in force.

37. C Systems substantially failed to perform, and thus materially breached, the Hosting Order, which required C Systems to “provid[e] update, maintenance and diagnostic services as part of your monthly hosting fee”, “maintain that software as well”, and “update the Software for [ACMG] when updates are available and considered stable and necessary.” The Hosting Order also warranted that C Systems would “provide [ACMG] with the same level of service we provide to others.”

38. Instead of “maintain[ing]” the services, C System allowed them to become vulnerable and exploited for multiple weeks; C Systems failed to “update the Software” with “available” and “necessary” patches; and C Systems did not provide ACMG with the “same level of service” it provided to others when it provided the critical patch to other clients but not to ACMG.

39. Likewise, the Master Consulting Agreement states that C Systems “will have access to certain trade secrets or other confidential information belonging to [ACMG], or belonging to third parties and which is in [ACMG’s] possession,” and obligated C Systems “not [to] disclose any such confidential information to any third party.” Exhibit C – Task Order to the Master Consulting Agreement states that “individual tasks will include: 1. Assist with the delivery and implementation of iMIS software, upgrades, and new releases. 2. Assist with day-to-day use, support, and configuration of the iMIS database... A C Systems project manager will be assigned to review all information systems needs.”

40. C Systems did not, in fact, properly perform these obligations when it allowed ACMG’s systems and data to become vulnerable and exploited for multiple weeks.

41. As a result of the breaches, the personal information of certain ACMG members and other users was potentially exposed to third parties, triggering over one hundred and fifty thousand dollars in damages for ACMG, including investigation costs, remediation of the Data Breach, the cost of notifying ACMG members and certain regulators of the Data Breach, and the cost of providing credit monitoring products.

42. As a result of C System’s breach of the Hosting Order and Master Consulting Agreement, ACMG is entitled to damages in an amount sufficient to reimburse ACMG for all costs incurred as a result of the Data Breach.

COUNT II – Breach of Covenant of Good Faith and Fair Dealing

43. ACMG incorporates each of the above allegations as if set forth fully herein.

44. New Jersey law implies a covenant of good faith and fair dealing in all contracts.

45. The implied covenant of good faith and fair dealing required that C Systems refrain from arbitrary or unreasonable conduct that has or had the effect of preventing ACMG from receiving the benefit of its bargain.

46. By reason of the conduct alleged in the foregoing paragraphs, C Systems has breached the implied covenant of good faith and fair dealing.

47. As a result, ACMG has been deprived of the opportunity to exercise its contractual rights and from receiving the benefit of its bargain, namely, the opportunity to operate its databases and website without intrusion of malicious attackers, such as occurred in connection with the Data Breach.

48. ACMG has suffered losses and damages in an amount that will be proven at trial, but reasonably believed to be over \$150,000 in costs and expenses incurred in connection with remediating the harm caused by the Data Breach.

COUNT III – Fraudulent Inducement

49. ACMG incorporates each of the above allegations as if set forth fully herein.

50. C Systems knowingly made false representations of material fact to ACMG, knowing such statements were false when making them, as detailed above, concerning the security and software updates, among others, with the intent of inducing ACMG in entering the Master Consulting Agreement and Hosting Order.

51. C Systems' response to ACMG's RFP, submitted to ACMG prior to entering the business relationship, states that C Systems' "premier hosting solution provides ... security

required for all customers to prevent network threats from getting in – and spreading.” A copy of C Systems’ response to the RFP is appended as Addendum A to the Master Consulting Agreement.

52. On November 7, 2016, for example, in response to ACMG’s question (“Is ongoing routine maintenance (e.g. OS security updates, patches) included?”), C Systems’ account manager wrote: “Yes, standard for all clients. Patch windows scheduled with you during on-board and security related updates pushed during this time. If Edge determines you are vulnerable and require an update outside of scheduled window we will notify you and alert of update with option to decline.”

53. ACMG reasonably relied upon C Systems’ statements before entering into the Master Consulting Agreement and Hosting Order, and had no reason to believe they were false.

54. As a result of C Systems’ conduct, ACMG has suffered damages in an amount sufficient to reimburse ACMG for all costs incurred as a result of the Data Breach.

COUNT IV – Negligent Misrepresentation

55. ACMG incorporates each of the above allegations as if set forth fully herein.

56. As discussed above, ACMG retained C Systems to develop and maintain ACMG’s databases and website.

57. In the course of seeking to be retained by ACMG, C Systems made material misrepresentations and/or omissions concerning, as detailed above, the security and software updates, among others, with the intent of inducing ACMG to enter into its relationship with C Systems.

58. ACMG reasonably relied upon ACMG’s material misrepresentations and/or omissions during the course of its relationship with C Systems, to its detriment.

59. As a result, ACMG has been and will continue to be damaged in an amount to be determined at trial.

COUNT V - Negligence

60. ACMG incorporates each of the above allegations as if set forth fully herein.

61. By maintaining the performance and security of ACMG's website, C Systems undertook a duty to use reasonable care to avoid causing foreseeable risk of harm to ACMG.

62. Moreover, C Systems' sole business purpose is to provide services such as those it promised to provide to ACMG, and C Systems holds itself out as an expert in providing such services.

63. As alleged herein, C Systems breached its duties by failing to act in accordance with a minimum standard of care in allowing an attacker to gain access to ACMG's website and servers maintained by C Systems and, thereby, facilitating that attacker's access to the personal information and payment card information of ACMG members and other users. In fact, as alleged herein, C Systems routinely notified ACMG of new releases of iMIS software patches for the first part of their business relationship; however, C Systems stopped doing this after the release of the October 2018 patch.

64. As a direct and proximate cause of C System's negligence, ACMG has suffered and will continue to suffer injury and damages as described herein.

COUNT VI – Violation of the New Jersey Consumer Fraud Act

65. ACMG incorporates each of the above allegations as if set forth fully herein.

66. The New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.*, ("CFA"), provides, in relevant part:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the

knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

N.J.S.A. 56:8-2.

67. C Systems engaged in unlawful practices under the CFS by making knowing misrepresentations and/or omissions to ACMG with the intent that ACMG would rely upon them in connection with the Master Consulting Agreement and Hosting Order, as discussed above.

68. C Systems' actions constitute misrepresentations, deception, fraud, false pretense, false promise, concealment, suppression, omissions, and/or unconscionable commercial practices under the CFS.

69. As a result of these unlawful practices, ACMG has suffered ascertainable loss, including the cost of remediating the harm suffered by the Data Breach.

70. The exact amount of the damages suffered by ACMG shall be determined at trial.

71. ACMG is also entitled to treble damages, counsel fees and costs under N.J.S.A. 56:8-19.

PRAYER FOR RELIEF

WHEREFORE, as a result of the foregoing, ACMG demands judgment in its favor and against C Systems, as follows:

A. Granting judgment in favor of ACMG on Count I, finding that Defendant C Systems materially breached the Master Consulting Agreement and Hosting Order by failing to provide and install software patches to ACMG's databases and website systems, and awarding ACMG judgment in an amount to be proven at trial representing the fees and costs incurred by

ACMG in connection with remediating the Data breach and pre-judgment interest accruing through and including the date of judgment;

B. Granting judgment in favor of ACMG on Count II, finding that Defendant C Systems has breached the implied covenant of good faith and fair dealing, and awarding ACMG judgment in an amount to be proven at trial, plus pre-judgment interest through and including to the date of judgment;

C. Granting judgment in favor of ACMG on Count III, finding that Defendant C Systems fraudulently induced ACMG to enter into the Master Consulting Agreement and Hosting Order, and awarding ACMG judgment in an amount to be proven at trial, plus pre-judgment interest through and including the date of judgment;

D. Granting judgment in favor of ACMG on Count IV, finding that Defendant C Systems made negligent misrepresentations to ACMG in order to induce it to enter into the Master Consulting Agreement and Hosting order, and awarding ACMG judgment in an amount to be proven at trial , plus pre-judgment interest through and including the date of judgment;

E. Granting judgment in favor of ACMG on Count V, finding that Defendant C Systems engaged in negligent conduct in performing services due to ACMG, and awarding judgment in an amount to be proven at trial, plus pre-judgment interest through and including the date of judgment;

F. Granting judgment in favor of ACMG on Count VI, finding that Defendant C Systems violated the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.*, by engaging in unlawful practices through misrepresentations, deception, fraud, false pretense, false promise, concealment, suppression, omissions, and/or unconscionable commercial practices that induced ACMG to enter into the Master Consulting Agreement and Hosting Order, and awarding

judgment in an amount to be proven at trial and trebled, plus pre-judgment interest though and including the date of judgment, plus counsel fees and costs pursuant to N.J.S.A. 56:8-19.

G. Awarding ACMG the fees, costs and expenses of this action; and

H. Granting ACMG such other and further relief, in law and in equity, as the Court may deem just and proper.

MCELROY, DEUTSCH, MULVANEY &
CARPENTER, LLP

Dated: February 12, 2021

By: /s/ Nicholas K. Lagemann
Nicholas K. Lagemann
1300 Mount Kemble Avenue
P.O. Box 2075
Morristown, New Jersey 07962-2075
(973) 993-8100
nlagemann@mdmc-law.com

SIDLEY AUSTIN LLP

Colleen T. Brown (*pro hac vice to be filed*)
1501 K. Street, N.W.
Washington, D.C. 20005
(202) 736-8000
ctbrown@sidley.com

Stephen W. McInerney (*pro hac vice to be filed*)
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
smcinerney@sidley.com

*Attorneys for Plaintiff American College of Medical
Genetics and Genomics.*

DEMAND FOR TRIAL BY JURY

ACMG respectfully demands a trial by jury on all issues so triable.

CERTIFICATION PURSUANT TO L. CIV. R. 11.2

I certify pursuant to 28 U.S.C. § 1746 that the foregoing matter in controversy is not the subject of any other pending lawsuit, arbitration or administrative proceeding, nor is any other such lawsuit or arbitration proceeding presently contemplated.

I understand that if any of the foregoing statements made by me are willfully false, I may be subject to punishment.

MCELROY, DEUTSCH, MULVANEY &
CARPENTER, LLP

By: /s/ Nicholas K. Lagemann
Nicholas K. Lagemann
Attorneys for Plaintiff

Dated: February 12, 2021